CLAIMS

What is claimed is:

1. A method of developing an access control list, comprising:

developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses;

converting at least one of,

user names into corresponding IP and physical addresses according to data in the enhanced access control list;

DNS names into corresponding IP addresses according to data in the enhanced access control list; and

physical addresses into IP addresses according to data in the enhanced access control list; and

developing the access control list from each of the operations of converting.

2. The method of claim 1 further comprising storing the user names and corresponding IP addresses in a mapping state database that defines current relationships among user names, DNS names, domain names, and physical addresses.

3. The method of claim 1 wherein each physical address comprises a MAC address.

4. The method of claim 1 wherein converting user names into corresponding IP and physical addresses according to data in the enhanced access control list comprises:

detecting 802.1x login packets being communicated over the network;

determining a MAC address from the 802.1x login packets;

detecting server message block login packets being communicated over the network; and

determining an IP address from the server message block login packets; and

developing records in the access control list using the obtained IP address for the respective user name.

5. The method of claim 1 wherein converting DNS names into corresponding IP addresses according to data in the enhanced access control list comprises:

detecting packets having an unknown source IP address;

generating a DNS name query using the source IP address;

receiving a DNS name associated with the IP address responsive to the query; and

developing records in the access control list using the obtained IP address for the respective DNS name.

6. The method of claim 5 further comprising occasionally generating new DNS name queries for the source IP address and thereafter repeating the operations of receiving and developing to update the access control list.

7. The method of claim 5 further comprising occasionally receiving the DNS name associated with the IP address and thereafter repeating the operation of developing to update the access control list.

8. The method of claim 1 wherein converting physical addresses into IP addresses according to data in the enhanced access control list comprises:

monitoring DHCP packets communicated over the network;

obtaining an IP address assigned to a particular physical address from the monitored DHCP packets; and

developing records in the access control list using the obtained IP address assigned to a respective physical address.

9. A method of controlling access of a user to a network including a plurality of hosts coupled together through a network switch, the method comprising:

storing in the network switch an enhanced access control list containing data related to at least one of user names, DNS names, Windows domain names, and physical addresses; and

generating a dynamic access control list from the enhanced access control list, the dynamic access control list containing a plurality of IP addresses that restrict access of the user to the network.

10. The method of claim 9 wherein generating the dynamic access control list comprises:

mapping user names to IP addresses;

mapping user names to physical addresses;

mapping physical addresses to IP addresses;

mapping unknown IP addresses to physical addresses; and

mapping unknown IP addresses to DNS names; and

applying rules set forth in the enhanced access control list relating to controlling access of a user to the addresses determined by the operations of mapping to generate the access control list.

11. The method of claim 10 wherein the physical addresses comprise MAC addresses.

12. The method of claim 10 wherein mapping user names to IP addresses comprises:

detecting server message block login packets being communicated over the network; and

determining an IP address from the server message block login packets.

13. The method of claim 10 wherein mapping user names to physical addresses comprises:

detecting 802.1x login packets being communicated over the network; and

determining a MAC address from the 802.1x login packets.

14. The method of claim 10 wherein mapping unknown IP addresses to DNS names comprises:

detecting packets having an unknown source IP address;

generating a DNS name query using the source IP address; and

receiving a DNS name associated with the IP address responsive to the query.

15. The method of claim 14 further comprising occasionally generating new DNS name queries for the source IP address and thereafter repeating the operations of generating and receiving.

16. The method of claim 10 wherein mapping unknown IP addresses to physical addresses comprises detecting packets having an unknown source IP address.

17. The method of claim 10 wherein mapping physical addresses to IP addresses comprises:

monitoring DHCP packets communicated over the network;

obtaining an IP address assigned to a particular physical address from the monitored DHCP packets.

18. A network switching circuit, comprising:

a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;

a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to store an enhanced access control list and a dynamic access control list; and

a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

19. The network switch of claim 18 wherein the processor further comprises a direct memory access controller coupled between the forwarding engine and the memory.

20. The network switch of claim 18 wherein the switch comprises an Ethernet switch and wherein the packets comprise Ethernet packets.

21. The network switch of claim 18 wherein the enhanced access control list comprises user names, DNS names, Windows domain names, and physical addresses.

22. A computer network, comprising:

a network switch, including,

a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;

a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to store an enhanced access control list and a dynamic access control list; and

a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets; and

a plurality of hosts, each host coupled to a respective port of the network switch.

23. The computer network of claim 22 wherein at least some of the hosts comprise personal computer systems.

24. The computer network of claim 22 wherein the network comprises an Ethernet network,, and wherein the switch comprises an Ethernet switch and the packets comprise Ethernet packets.

25. The computer network of claim 22 wherein the enhanced access control list comprises user names, DNS names, Windows domain names, and physical addresses.